Dor: https://dorl.net/dor/20.1001.1.28212606.1403.7.3.3.5

فصلنامهٔ آماد و فناوری دفاعی، سال هفتم، شماره ۳ (پیاپی ۲۳)، پاییز ۱۴۰۳

مطالعه مقایسه‌ای قوانین سایبری چین، ایالات متحده آمریکا و روسیه؛ بایسته‌ها و ضرورت‌های امنیت سایبری جمهوری اسلامی ایران

روح‌اله ملکی عزین‌آبادی*[۱]، جواد جمالی[۲]

تاریخ دریافت: ۱۴۰۳/۰۲/۱۰ **پذیرش مقاله: ۱۴۰۳/۰۲/۲۶**

چکیده

بهره‌گیری از فضای سایبر به‌عنوان شیوه‌ای نوین برای تهاجم، از قالب انتزاعی در دنیای مجازی به واقعیتی عینی و جدی در عصر حاضر تبدیل شده است که به‌صورت فراگیر موجبات دغدغه و نگرانی دولت‌ها و سازمان‌های نظامی و امنیتی ملی، منطقه‌ای و بین‌المللی را فراهم آورده است. فراوانی رخداد این نوع از حملات که روزبه‌روز افزایش یافته و اشکال گسترده‌تر و پیچیده‌تری به خود می‌گیرد، زنگ خطری برای دولت‌ها و در نهایت جامعه بین‌المللی تلقی می‌شود که ضرورت و اهمیت پرداختن به آن را جدی‌تر ساخته است. جمهوری اسلامی ایران تاکنون مورد هدف گسترده‌ترین و پیچیده‌ترین این نوع از حملات قرارگرفته است؛ بنابراین، کنکاش و جستار در جوانب امنیتی حملات و تهدیدات سایبری می‌تواند زمینه‌ساز ایجاد یک چارچوب منسجم و یکپارچه برای ج.ا.ایران در سطح دفاعی و امنیتی باشد. در این راستا و برای مقابله با انواع تهدیدات سایبری، این پژوهش با بررسی مقایسه‌ای قوانین سایبری چین، ایالات متحده امریکا و روسیه، خواستار ارائه راهکارهای عملیاتی برای ج.ا.ایران می‌باشد. برای تحقق این امر از روش تحقیق مطالعه تطبیقی بهره گرفته می‌شود و استدلالات به صورت استنادی-موردی می‌باشد.

واژگان کلیدی: تهدیدات سایبری، امنیت سایبری، چین، ایالات‌متحده امریکا، روسیه، ج.ا.ایران.

۱. دانش‌آموخته دکتری روابط بین‌الملل دانشگاه تهران، تهران، ایران، رایانامه: *r.malaki1991@gmail.com*.

۲. دانش‌آموخته دکتری جامعه‌شناسی سیاسی دانشگاه علامه طباطبایی، تهران، ایران، رایانامه: *jamalijavad76@yahoo.com*.

۱. مقدمه

اینترنت دولت‌ها را در مقابل چالش‌های جدید امنیتی قرار داده است. هزینه کم ورود، ناشناس‌بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری موجب گردید تا کنشگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته، تروریستی و حتی افراد به این فضا وارد شده و تهدیدهایی زیر را به وجود آورند:

(۱) جنگ سایبری،

(۲) جرائم سایبری،

(۳) تروریسم سایبری،

(٤) جاسوسی سایبری و... .

همین نکته، تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی برخوردار هستند و کنشگران آن را دولت- ملت‌هایی تشکیل می‌دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است که امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شود و ناکارآمد به حساب آید.

بنابراین، به‌نظر می‌رسد طرح موضوع حملات سایبری در فضای سایبر به‌عنوان پدیده‌ای نوین و چالشی جدی فراروی دولت‌ها در عصر و هزاره جدید ارتباطات و فناوری‌های نوین اهمیت و ضرورتی دوچندان یافته است. بنابراین، تحقق امنیت سایبری به عنوان یکی از مهم‌ترین دغدغه‌های تمامی دولت‌ها از جمله قدرت‌های بزرگی نظیر چین، آمریکا و روسیه است که نزدیک به دو دهه می‌باشد که در این زمینه به قانون‌گذاری و سرمایه‌گذاری می‌پردازند. از آنجایی‌که ج.ا.ایران همواره با تهدیدات سایبری روبرو می‌باشد و پس از تجربه تلخ حمله ویروس «استاکس‌نت»[1]، لزوم طرح‌ریزی مدلی همه‌جانبه براساس موازین حقوق بین‌الملل و تصویب قوانین داخلی جهت ارتقای امنیت سایبری را بیش از پیش احساس می‌شود.

1. Stuxnet

۲. مبانی نظری و پیشینه‌شناسی تحقیق

۲-۱. پیشینه‌شناسی

در مورد پیشینه پژوهش، مقاله یا پژوهشی که به‌طور مستقیم به این موضوع پرداخته باشد، یافت نشد. اما می‌توان به برخی از پژوهش‌ها در منابع داخلی و منابع لاتین که در ارتباط با این موضوع صورت گرفته و از حیث برخی از معانی و مفاهیم نیز می‌تواند نگارندگان را در پیشبرد اهداف این تحقیق یاری رساند، اشاره نمود.

«جار پریر»[1] در پژوهشی با عنوان «استیلای ترند: رسانه‌های اجتماعی به‌مثابه جنگ اطلاعاتی» (۲۰۱۷) که در فصلنامه مطالعات استراتژیک منتشر کرده است، به این موضوع اشاره دارد که رسانه‌های اجتماعی به‌عنوان ابزاری برای نبردهای اطلاعاتی بدل شده‌اند. از دیدگاه نویسنده، متقاعدسازی کاربران از طریق انتشار پیام‌های سیاسی و تبدیل آن به یک ترند، از ابزارهای مهم نبردهای اطلاعاتی می‌باشد که کشورهای قدرتمند از آن علیه رقبا و دشمنان خود بهره می‌گیرند.

«محمدی خانقاهی و آزادی» در مقاله‌ای تحت عنوان «تفاوت‌های امنیت سایبری اجتماعی با امنیت سایبری» (۱۴۰۰) به بررسی حملات سایبری علیه شهروندان یک جامعه می‌پردازند. از دیدگاه نویسندگان، دشمنان ج.ا.ایران تلاش می‌کنند از رسانه‌های اجتماعی به عنوان ابزاری برای بی‌اعتبار کردن سیستم حکومتی و نهادهای مرتبط با آن بهره گیرند. ازاین‌رو، مخالفان نظام سیاسی ایران می‌کوشند از فضای سایبری برای انتشار اخبار جعلی بهره گیرند تا امنیت روانی جامعه را با تهدید مواجه سازند.

«زواره‌ای و سلیمی» در مقاله‌ای تحت عنوان «اعمال صلاحیت جهانی بر جرائم علیه امنیت سایبری در هوانوردی بین‌المللی» (۱۴۰۱) به بررسی اقدامات و خرابکاری‌های سایبری در حوزه هوانوردی بین‌المللی می‌پردازند که دربرگیرنده هواپیماربایی و تروریسم سایبری می‌باشد. از دیدگاه نویسندگان، اعمال صلاحیت جهانی یک مکانیسم بازدارنده

1. Jarred Prier

می‌باشد که می‌تواند پشتیبان مبارزه علیه امنیت سایبری باشد و سبب بی‌کیفر ماندن مجرمین این جرم گردد.

۲-۲. مبانی نظری و مفهوم‌شناسی تحقیق

۱-۲-۲. امنیت سایبری

مفهوم «امنیت سایبری» یک مؤلفه مهم در زیرساخت‌های کشور است. امنیت سایبری در مفهوم سنتی به جلوگیری از «هک» فناوری دستگاه‌های اطلاعاتی اشاره دارد. این مفهوم در معنای جدید خود، علاوه‌بر این‌که مفهوم گذشته را شامل می‌شود، به جلوگیری از هک انسان‌ها که گاهی اوقات از آن به عنوان «هک شناختی» یاد می‌شود، نیز اشاره دارد. در مجموع، امنیت سایبری را می‌توان تحت عنوان «حفاظت از زیرساخت‌های اطلاعاتی مهم و فرآیندها و محتوای آن» تعریف نمود (تئوهاری[1]،۲۰۱۸: ۲۳).

این مفهوم دربرگیرنده محافظت از سیستم‌ها، شبکه‌ها، برنامه‌ها و سامانه‌های نرم‌افزاری در برابر حملات دیجیتالی می‌باشد. هدف از امنیت سایبری، «محافظت از اطلاعات در برابر سرقت و آسیب» است. بدون وجود امنیت سایبری، سازمان‌ها نمی‌توانند از خود در برابر نقض‌های داده‌ها و حمله‌های هکرها دفاع کنند و به هدفی ساده برای مجرمان سایبری تبدیل می‌شوند (انوشا و همکاران، ۱٤۰۰: ۳)

۲-۲-۲. مفاهیم مرتبط با امنیت سایبری

با مطالعه در متونی که در حوزه امنیت سایبری منتشر شده است، این مفهوم به‌طور مشخص با برخی از مفاهیم اساسی ارتباط تنگاتنگی دارد؛ به‌گونه‌ای که مهم‌ترین مفاهیم مرتبط با این حوزه را می‌توان شامل موارد ذیل دانست.

۱-۲-۲-۲. تهدید سایبری

«تهدید سایبری» عبارت است از هر اقدامی که بتواند امنیت شبکه و سیستم را به منظور هدفی خاص مورد خدشه قرار دهد. اهداف تهدید سایبری به سه سطح تقسیم می‌شوند:

1. Theohari, C. A.

- ❖ در سطح اول، معمولاً افراد مورد هدف قرار می‌گیرند و اقداماتی از قبیل: «سرقت هویت» یا «دسترسی غیرمجاز به اطلاعات شخصی به منظور باج خواستن از فرد قربانی» را که بیشتر رنگ و بوی مالی دارند، شامل می‌شود.
- ❖ سطح دوم، دولت‌ها هستند که هدف، «آسیب رساندن به زیرساخت‌های حیاتی یا جاسوسی از آن‌ها با انگیزه‌های سیاسی» است.
- ❖ در سطح سوم، شرکت‌های بزرگ غیردولتی قرار دارند که هدف از آن، ترکیبی از سطح اول و سطح دوم است.

تهدیداتی که در سطح فردی صورت می‌گیرند، در بیشتر مواقع در دسته جرائم سایبری قرار می‌گیرند. تهدیداتی که در سطح دوم و سوم قرار می‌گیرند، جنبهٔ حمله سایبری دارند. این تهدیدات در قالب حوادث که صورت فنی دارند، از حالت بالقوه به حالت بالفعل در می‌آیند (رهامی و اژدری، ۱٤۰۱: ۲۲۷).

۲-۲-۲-۲. حوادث سایبری

تهدیدات سایبری در قالب حوادث سایبری ظهور و بروز می‌یابند. به‌عبارتی، در قالب این حوادث می‌باشد که تهدیدات سایبری از قوه به فعل در می‌آیند. از مهم‌ترین حوادث سایبری می‌توان به موارد زیر اشاره کرد:

(۱) نشت اطلاعاتی،

(۲) جاسوسی سایبری،

(۳) هرزنامه سرقت هویت افراد،

(٤) ویروس‌های اینترنتی،

(۵) دستکاری اطلاعاتی،

(٦) مواردی نظیر سرقت رمز ارز و فیشینگ.

۳-۲-۲-۲. جرائم سایبری

جرائم سایبری به جرائمی گفته می‌شود که در محیطی غیر فیزیکی علیه فناوری اطلاعات با حالت شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابد (بیابانی و هادیانفر، ۱۳۸٤: ۱۸۳). در این

نوع از جرائم نیز از تلفن، اینترنت و فضای مجازی به‌عنوان ابزارهایی برای ارتکاب جرائمی نظیر کلاه‌برداری، سرقت و تجاوز استفاده می‌شود.

٤-۲-۲-۲. حمله سایبری

«جنگ سایبری» نوعی جنگ است که دولت‌ها در آن بازیگر اصلی می‌باشند و توسط آنان رهبری و هدایت می‌گردند تا از این طریق؛ امکانات، توانایی‌ها، تأسیسات و نقاط قوت دشمن را تخریب نمایند و دشمن را در برابر خواسته‌های خود تسلیم کنند (لی[1]، ۲۰۱۳: ۹۹-۱۱۳). علی‌رغم آن‌که در این جنگ، دولت‌ها از کنشگران غیردولتی، ارتش سایبری و هکرهای خود بهره می‌گیرند، اما بازیگر و راهبر اصلی آن، دولت‌ها می‌باشند.

موفقیت در این حوزه‌ها به توانایی و استراتژی یک کشور در ارتقای امنیت سایبری و محافظت از اطلاعات و داده‌های مرتبط با آن در مقابل افراد، گروه‌ها و نهادهایی که قصد سوءاستفاده از آن را دارند، بستگی دارد.

اتخاذ یک استراتژی امنیت سایبری مؤثر در برابر این حملات خرابکارانه که به هدف دسترسی، تخریب، حذف و کنترل سیستم‌های کاربران صورت می‌گیرد، می‌تواند کشور را در مقابله با این تهدیدات در یک وضعیت مناسب قرار دهد. بهره‌گیری از تجارب کشورهای موفق در این حوزه از طریق بررسی استراتژی امنیت ملی آن‌ها می‌تواند گام مؤثری در ارتقای امنیت سایبری کشورها باشد.

۳. روش‌شناسی تحقیق

روش پژوهش حاضر، کیفی و از نوع توصیفی-تحلیلی می‌باشد. این تحقیق به لحاظ هدف «توسعه‌ای- کاربردی» می‌باشد. داده‌های این پژوهش می‌تواند به لحاظ کاربردی، برای ارتقای امنیت سایبری ج.ا.ایران مؤثر باشد. روش گردآوری اطلاعات، «اسنادی و کتابخانه‌ای» می‌باشد. داده‌های به‌دست‌آمده با استفاده از روش «تحلیل مضمون» مورد بررسی قرار گرفته و در قالب جداول ارائه گردید.

1. Lee, D.

٤. تجزیه‌وتحلیل یافته‌ها

بسیاری از کشورها در سطح ملی اقدام به تهیه و تدوین سیاست‌ها، استراتژی‌ها و بعضاً قوانین و مقررات ملی برای حفاظت از فضای ملی سایبری خود و همچنین مقابله با تهدیدهای بالقوه ناشی از ارتکاب حملات سایبری کرده‌اند. از جمله مهم‌ترین کشورهایی که در این حوزه اقدام به تدوین سیاست‌ها و استراتژی نموده‌اند، می‌توان به چین، آمریکا و روسیه اشاره کرد که در ادامه به آن‌ها اشاره می‌شود.

٤-١. قوانین سایبری چین

چین پس از تحقق اهمیت اطلاعات رایانه‌ای در توسعه اقتصادی خود، توسعه سریع آن را مورد پیگیری قرار داد توسعه اینترنت در کشور چین با کنترل و تنظیم شدید دولت بر زیرساخت‌های اینترنت، استفاده تجاری، اجتماعی و نتایج سیاسی آن همراه بود (لیانگ و لو[1]، ۲۰۱۰: ۱۰۳-۱۲۰). قوانین و مقررات مختلف، این موضوع را که در چه شرایطی فعالیت‌ها و اطلاعات مختلف آنلاین غیرقانونی تلقی می‌شوند را تبیین می‌کند (کمیسیون اجرایی کنگره درباره چین[2]، ۲۰۰۵). مهم‌ترین بخش‌های این قوانین عبارت‌اند از:

(۱) نقص اصول بنیادین که در قانون اساسی مورد تأیید قرار گرفته‌اند؛

(۲) به خطر انداختن امنیت ملی، افشای اسرار دولتی، براندازی رژیم ملی یا به‌طورکلی به‌خطر انداختن یکپارچگی وحدت ملی؛

(۳) آسیب‌رساندن به قداست منافع ملت؛

(٤) تحریک دشمنی علیه ملت، نژادپرستی یا اختلال در همبستگی ملی؛

(۵) اختلال در سیاست‌های ملی در مورد دین، ترویج فرقه‌های شیطانی و خرافه‌پرستی؛

(٦) انتشار شایعات، اخلال در نظم اجتماعی یا مختل کردن ثبات اجتماعی؛

(۷) ترویج پورنوگرافی، قمار، خشونت، ترور و یا ارتکاب جرم؛

1. Liang, B.; Lu, H.
2. Congressional Executive Commission on China (2005)

(۸) توهین به شخص ثالث یا نقض حقوق قانونی و منافع آن‌ها؛

(۹) تحریک مجامع، انجمن‌ها، راهپیمایی‌ها، تظاهرات یا تجمعات غیرقانونی که نظم اجتماعی را مختل می‌کند؛

(۱۰) انجام فعالیت تحت نام سازمان‌های غیرقانونی مدنی؛

(۱۱) و مطالب دیگری که توسط قانون ممنوع است.

این شرایط مستقیماً بنیانی را شکل می‌دهد که سیاست‌هایی از طریق آن اعمال می‌گردد که در آن‌ها هم حقوق دیجیتالی را نقض می‌کند و هم از آن‌ها محافظت می‌کند. به‌نظر می‌رسد این شرایط از یک‌طرف حمایت از حقوق مختلف مانند حقوق اقلیت‌ها (بند ٤) و حقوق کودکان را تضمین می‌کند (بند ۷).

در سال ۱۹۹۸م. پروژه «گلدن شیلد»، که امروزه بیشتر با عنوان فایروال[1] بزرگ چین شناخته می‌شود، توسط وزارت امنیت عمومی راه‌اندازی شد. آنچه به‌عنوان بزرگ‌ترین فایروال جهان شناخته می‌شود، یک پروژه نظارتی ترکیبی است که از فایروال، ثبت‌نام اینترنتی، فیلتر کلیدواژه‌ها، کنترل دولتی بر وب‌سایت‌ها برای ایجاد محدودیت سایبری در اینترنت چین استفاده می‌کنند (شو و آلبرت[2]، ۲۰۱۷). کاربرد اصلی این پروژه، انجام کنترل و نظارت بر اطلاعات در اینترنت (در سطح داخلی و خارجی) است (داول[3]، ۲۰۰٦: ۱۱۹- ۱۱۱).

درحالی‌که استفاده از وی‌پی‌ان در گذشته راحت بود، اما در سال ۲۰۱۸م. در گزارش خانه آزادی آمده است که دولت چین اقدامات جدیدی را برای محدود کردن استفاده از ابزارهای دور زدن فیلترینگ انجام داده است (خانه آزادی[4]، ۲۰۱۸). حتی شرکت‌های خارجی که در سرزمین چین فعالیت می‌کنند، تحت فشار قرار گرفتند تا از کمک به دور زدن فیلترینگ خودداری کنند.

1. Firewall
2. Xu, B.; Albert, A.
3. Dowell, W.
4. Freedom House

علاوه‌بر این، «سیستم اعتبار اجتماعی» برای نخستین بار در سال ۲۰۱٤م. دنبال شد. این سیستم، رفتارهای شهروندی و آفلاین افراد را کنترل و سپس تعیین می‌کند که شهروندان چه مزیت‌ها و محدودیت‌هایی متناسب با رفتارشان خواهند داشت. به‌طور مثال، افرادی که دارای رتبه‌بندی باشند، ممکن است محدودیت‌های چون ممنوعیت سفر هوایی و ریلی بر آن‌ها تحمیل شود و افراد با رتبه خوب دارای مزیت‌هایی چون دسترسی به امنیت و معافیت از پرداخت در هتل بهره‌مند شود (شاهباز[1]، ۲۰۱۸). علاوه بر نقض حریم خصوصی و آزادی بیان، این قانون به نقض حق جنبش متهم شده، بنابراین دامنه حقوق بشر تحت تأثیر اینترنت قرارگرفته است. در جدول (۱) قوانین و مقررات عمده چین در حوزه مسائل سایبری ارائه شده است (نک: عفو بین‌الملل[2]، ۲۰۱۸؛ ژیرارد[3]، ۲۰۱۸؛ شاهباز[4]، ۲۰۱۸؛ کمیته دائمی NPC[5]؛ خانه‌آزادی[6]، ۲۰۱۸)

جدول شماره ۱. قوانین و مقررات عمده چین

قوانین و مقررات	تاریخ	هدف
قانون جزایی جمهوری خلق چین	مارس ۱۹۹۷	آنچه مخل امنیت ملی، امنیت عمومی و بازار سوسیالیستی باشد، جرم می‌داند. اصلاحات بعدی جرائم سایبری را نیز شامل می‌شود.
تدابیر مربوط به مدیریت حفاظت از امنیت شبکه بین‌المللی اطلاعات کامپیوتر	دسامبر ۱۹۹۷	محافظت از شبکه اطلاعات بین‌المللی، نظم عمومی و ثبات اجتماعی با تشریح فعالیت‌های غیرمجاز در شبکه‌های بین‌المللی.
تدابیر مربوط به مدیریت سرویس‌های اطلاعات اینترنت	سپتامبر ۲۰۰۰	تنظیم فعالیت‌های سرویس اطلاعات اینترنت به‌وسیله الزام سرویس‌های اطلاعات اینترنت به کسب اجازه از دولت.
		با تنظیم مقررات راه دور، قوانین قبلی را به‌گونه‌ای

1. Shahbaz, A.
2. Amnesty International (2018)
3. Girard (2018)
4. Shahbaz, A.
5. NPC StandingCommittee (2000)
6. Freedom House (2018)

مقررات مربوط به ارتباطات راه دور مردم جمهوری چین	نوامبر ۲۰۰۰	گسترش می‌دهد که صدا، متن، اطلاعات، تصاویر و سایر اطلاعات که از سیستم‌های وایرلس استفاده می‌کنند را شامل شود. قوانین مدیریت سرویس‌های بولتن‌های الکترونیکی: تنظیم محتوا، دوره نگهداری و نوع بولتن‌های الکترونیکی.
تصمیم کمیته کنگره ملی حفظ امنیت اینترنت	دسامبر ۲۰۰۰	نحوه استفاده از اینترنت را در راستای توسعه منافع چین تعریف می‌کند.
مقررات مربوط به مدیریت شرکت‌های ارتباطی خارجی سرمایه‌گذاری	دسامبر ۲۰۰۱	شرکت‌های سرمایه‌گذار خارجی را ملزم به رعایت قوانین و مقررات ملی برای انجام تجارت در چین می‌کند.
قوانین مدیریت سرویس‌های خبری اینترنت	سپتامبر ۲۰۰۵	تنظیم سرویس‌های اطلاعاتی خبری اینترنتی در راستای تأمین منافع ملی و عمومی. هیچ سرویس خبری بر مبنای سرمایه‌گذار خارجی نمی‌تواند تأسیس شود.
قانون امنیت سایبری	ژوئن ۲۰۱۷	متمرکز کردن خط‌مشی اینترنت و الزام شرکت‌های اینترنتی برای سانسور محتوای کاربران، محدود کردن ناشناسی آنلاین، متمرکز کردن اطلاعات شخصی.
قانون اطلاعات ملی	جولای ۲۰۱۷	افراد، سازمان‌ها و نهادها را موظف می‌کند تا با جاسوسی و گزارش‌دادن به مقامات امنیت عمومی و دولتی کمک کنند. به‌علاوه اجازه دسترسی به هرگونه اطلاعات در رسانه‌های اجتماعی را به دولت می‌دهد.

۲-٤. قوانین سایبری روسیه

روسیه دارای یک تاریخچه طولانی و پیچیده در ارتباط با اطلاعات است. در روزگار اتحاد جماهیر شوروی، اطلاعات و رسانه‌ها به‌شدت کنترل می‌شدند تا جایی‌که مالکیت و استفاده دستگاه‌های کپی نیز توسط دولت تنظیم می‌شد (مدرسه سیاست عمومی CEU[1]، ۲۰۱۷).

1. CEU School of Public Policy (2017)

مطابق گزارش آزادی اینترنت در سال ۲۰۱۸م.، مجازات‌هایی برای فعالیت اینترنتی مختلف در روسیه وضع شده است که عبارت‌اند از:

(۱) بدنامی عمومی،

(۲) افترا علیه قاضی یا دادستان،

(۳) توهین به مقامات،

(٤) فراخوان برای تروریسم،

(۵) توهین به احساسات مذهبی،

(٦) فراخوان افراط‌گرایی،

(۷) جدایی‌طلبی،

(۸) ترویج نفرت،

(۹) انتشار اطلاعات نادرست در مورد فعالیت‌های جنگ دوم جهانی.

به‌علاوه قانون اداری روسیه برای دو فعالیت دیگر مجازات‌هایی را تعیین می‌کند:

الف. نمایش نمادهای نازی یا سمبل‌های سازمان‌های افراطی،

ب. انتشار مواد و ابزارهای افراطی‌گری (خانه آزادی، ۲۰۱۸).

لیست سیاه وب‌سایت‌ها، ابزاری رایج در دست دولت روسیه برای کنترل و نظارت بر سایت‌های اینترنتی است. تعداد این وب‌سایت‌ها در طول سالیان گذشته همواره درحال افزایش بوده است. در بین سال‌های ۲۰۱۲م. تا ۲۰۱۳م. اصلاحات قانون فدرال به روسکومندزور و سایر آژانس‌ها اجازه تصمیم‌گیری در مورد مسدود شدن وب‌سایت‌ها را داده است. سازمان روسکومندزور فهرستی از وب‌سایت‌های مسدود شده را دارد که طبق ادعای مقامات شامل محتوای کودک‌آزاری، مواد مخدر، خودکشی، نقض حق چاپ، فراخوان برای اقدام عمومی و ... هستند. همانند سانسور چین، برای توجیه مجدد کنترل بر محتوای اینترنت قانونی را در مورد حقوق کودکان تصویب کرد (جیمز و جونز[1]، ۲۰۱۷). این نوع سانسورها، توسط ارائه‌دهندگان خدمات اینترنت تأیید می‌شود که باید به لیست

1. James, Y.; Jones, S.

سیاه روسکومندزور مراجعه کنند. به‌علاوه ارائه‌دهندگان خدمات اینترنتی حق تعیین سیاست‌هایی برای چگونگی محدود شدن دسترسی در فیلترهای تصادفی را ندارند. در نتیجه ۹۷ درصد انسدادهای تصادفی ناشی از مسدود شدن IP به‌جای نام وب‌سایت بوده است (خانه آزادی، ۲۰۱۸). در جدول (۲) قوانین و مقررات عمده روسیه در حوزه مسائل سایبری ارائه شده است[1] (نک: خانه آزادی، ۲۰۱۸ و ۲۰۱۷؛ مارشال، ۲۰۱۷؛ نوستی، ۲۰۱۵).

جدول شماره ۲. قوانین و مقررات عمده روسیه

قوانین و مقررات	تاریخ	هدف
قانون نمایندگان خارجی	جولای ۲۰۱۲	سازمان‌های غیردولتی ثبت‌شده که بودجه خارجی دریافت می‌کنند و مشمول فعالیت‌هایی هستند که به نظر سیاسی تلقی می‌شود به عنوان نماینده خارجی به حساب می‌آیند و تحت حسابرسی قرار می‌گیرند.
قانون فناوری و امنیت اطلاعات (اصلاحات)	فوریه ۲۰۱٤	اجازه مسدودسازی سایت‌هایی را می‌دهد که اقدام به شورش و اقدامات تروریستی افراطی می‌کنند. قانون را به مبارزه با پورنوگرافی کودکان گسترش می‌دهد. جدیدترین اصلاحات برای ذخیره اطلاعات کاربر در روسیه به خدمات اینترنتی خارجی نیازمند است.
تدابیر مربوط به مدیریت سرویس‌های اطلاعات اینترنت	سپتامبر ۲۰۰۰	تنظیم فعالیت‌های سرویس اطلاعات اینترنت به وسیله الزام سرویس‌های اطلاعات اینترنت به کسب اجازه از دولت.
قانون وبلاگ نویسان	آگوست ۲۰۱٤	کلیه رسانه‌های آنلاین از جمله وبلاگ‌ها و صفحات شخصی با شبکه‌های اجتماعی بیش از ۳۰۰۰ بازدیدکننده روزانه باید در روسکومندزور (نهاد تنظیم‌کننده رسانه‌های جمعی) ثبت‌نام کنند.
قانون رسانه جمعی (اصلاحات)	ژانویه ۲۰۱٦	اتباع و سازمان‌های خارجی نمی‌توانند بیش از بیست درصد سهام رسانه‌های روسی را در اختیار داشته

1. Sources: Freedom House, 2018; Maréchal, 2017; Nocetti, 2015; & Freedom House, 2017.

		باشند. قانون در مورد جمع‌آوری اخبار: موتورهای جستجوگر با بیش از یک میلیون کاربر باید روزانه صحت اطلاعات را قبل از انتشار برای عموم بررسی کنند. خبرهایی که دروغ تلقی می‌شوند باید از وب‌سایت‌ها حذف شوند در غیر این صورت با مجازات‌های مالی رو می‌شوند که این امر باعث خودسانسوری شرکت‌های خصوصی و جریان آزاد اطلاعات می‌شود.
قانون یاروویا	جولای ۲۰۱۸	ارائه خدمات آنلاین برای تهیه کلیدهای رمزگذاری موظف است پرونده‌ها را به مدت شش ماه نگه داشته و هرگونه اطلاعاتی که دولت فدرال خواستار باشد را ارائه دهد. این امر حریم خصوصی شهروندان و توانایی ابراز مخالفت سیاسی را محدود می‌کند.

۳-٤. قوانین سایبری ایالات متحده آمریکا

در ایالات متحده آمریکا، حق آزادی بیان و مطبوعات توسط اولین اصلاحیه قانون اساسی به رسمیت شناخته شده است. در سال ۱۹۹۷م. دادگاه عالی اتحادیه آزادی‌های مدنی آمریکا به اتفاق آرا اولین اصلاحیه برای محافظت از گفتار آنلاین را تصویب کرد. این تصمیم قانون صیانت از ارتباطات در ۱۹۹٦م. را فراهم کرد که اولین تلاش قابل‌توجه در زمینه تنظیم انتشار مطالب پورنوگرافی آنلاین، برخلاف قانون اساسی و پیش‌زمینه مباحث بعدی در مورد سانسور آنلاین بود. به همین ترتیب، دادگاه‌ها در طول سال‌ها بارها و بارها اقدام به‌تنظیم محتوای آنلاین کرده‌اند. درنتیجه، خانه آزادی به‌طور مداوم ایالات‌متحده را در گزارش‌های سالانه خود از سال ۲۰۱۱م. ارزیابی کرده است. با این‌حال، نمره آزادی اینترنت ایالات‌متحده از سال ۲۰۱۱م. تا ۲۰۱۸م. از ۱۳ به ۲۲ افزایش یافته است که از روند روبه وخامت آن حکایت دارد (قانون آمریکا[1]، ۲۰۱۹).

1. Us Legal

این موضوع حکایت از آن دارد که ایالات متحده آمریکا به این نتیجه راهبردی رسیده است که تنها راه مقابله با تهدیدات سایبری، کنترل و مدیریت فعالیت‌های سایبری است. از سویی دیگر، قوانین حاکم بر سایر جنبه‌های زندگی مدنی به‌طور فزاینده به اینترنت گسترش یافته است که شامل موارد زیر می‌شود:

(۱) نقض حق چاپ،

(۲) پورنوگرافی کودکان،

(۳) مطالبی که برای افراد زیر سن قانونی مضر هستند،

(٤) قمار،

(۵) جرائم مالی (خانه آزادی، ۲۰۱۱).

در جدول (۳) قوانین و مقررات عمده ایالات متحده آمریکا در حوزه مسائل سایبری ارائه شده است.[1]

جدول شماره ۳. قوانین و مقررات عمده ایالات‌متحده آمریکا

قوانین و مقررات	تاریخ	هدف
فرمان اجرایی	دسامبر ۱۹۸۱	پایه و اساس چگونگی عملکرد NSA و سایر آژانس‌های فدرال برای نظارت را برای نظارت بر جمعیت در ایالات‌متحده فراهم کرده است. قانون میهن‌پرستی: زمانی که تحقیقات مربوط به تروریسم بین‌المللی باشد، بدون نیاز به حکم قبلی، تمامی دستگاه‌های ارتباطی از تلفن‌ها گرفته تا اینترنت و ایمیل را می‌شود بررسی کرد.
قانون حمایت از اینترنت کودکان	اکتبر ۲۰۰۱	کتابخانه‌ها برخی مدارس را ملزم می‌کند تا نرم‌افزار فیلترکردن محتوا را بر روی رایانه‌های خود نصب کنند تا دسترسی به محتوای خاصی از جمله مستهجن و دستورالعمل ساخت بمب را مسدود کند. این نرم‌افزار به‌طور ناخواسته انواع مختلف گفتار ازجمله:

1. Sources: Gellman and Soltani, 2014; Homeland Security Act, 2002; Bazan, 2004; Butler, 2015; Keane and Swire, 2018; & Freedom House, 2018.

		کمدی، مراقب‌های شخصی، اشعار کوتاه و سایت‌های بهداشت را مسدود می‌کند.
قانون امنیت ملی	نوامبر ۲۰۰۲	وزارت امنیت ملی را تأسیس می‌کند. اختیار را به وزیر امنیت ملی می‌دهد تا تحقیقات لازم را برای هدایت و کنترل تحقیقات لازم برای جلوگیری از تروریسم انجام دهد.
اصلاحات اطلاعاتی و قانون پیشگیری از تروریسم	دسامبر ۲۰۰٤	دفتر نظارت بر اداره اطلاعات ملی را برای نظارت بر جامعه اطلاعاتی تأسیس کرد. بخش ٦۰۰۱ تعریف عامل قدرت خارجی در FISA را اصلاح می‌کند و ماده «گرگ تنها» را در اشاره به شهروند خارجی مرتبط با تروریسم بین‌الملل اضافه می‌کند. ازاین‌رو، روند اعمال حکم دادگاه را تسهیل می‌کند.
بند ۷۰۲ اصلاح قانون نظارت بر اطلاعات خارجی	جولای ۲۰۰۸	به NSA اجازه جمع‌آوری داده‌های ارتباطی کاربران به همراه محتوای آن را از شرکت‌های فناوری ایالات‌متحده، از طریق زیرساخت‌های فیزیکی را می‌دهد. اجازه نظارت مستقیم بر ارتباطات اتباع بیگانه و غیرمستقیم بر شهروندان ایالات‌متحده را می‌دهد.
قانون آزادی ایالات‌متحده	ژوئیه ۲۰۱۵	تمدید مفاد مقتضی قانون میهن‌پرستی بدون تغییر قابل‌توجه در رویه‌های نظارت جمعی.
قانون به اشتراک‌گذاری اطلاعات امنیت سایبری	دسامبر ۲۰۱۵	شرکت‌های آمریکایی را از شکایت در مورد نقض حریم خصوصی کاربران در هنگام به اشتراک‌گذاری اطلاعات با آژانس‌های فدرال حمایت می‌کند. از وزارت امنیت می‌خواهد تا درباره تهدیدات اطلاعات به شرکت‌های خصوصی بگوید. اما با این انتقاد نیز مواجه است که درباره این‌که چه زمانی می‌توان از داده‌ها برای امنیت یا اجرای قانون استفاده کرد به‌طور واضح مشخص نکرده است.
قانون شفاف‌سازی استفاده از اطلاعات	مارس ۲۰۱۸	به‌روزرسانی قانون ذخیره ارتباطات ۱۹۸٦ با روشن کردن نحوه انتقال داده‌های فراملی. قانون دسترسی به اطلاعات را صرف‌نظر از این‌که این اطلاعات در خارج یا داخل کشور ذخیره شده‌اند، گسترش

		می‌دهد.
قانون اجازه به ایالات و قربانیان برای مبارزه با قاچاق جنسی آنلاین	آوریل ۲۰۱۸	اعمال مجازات بر وب‌سایت‌های که باعث فحشا قاچاق جنسی می‌شوند.

٤-٤. چالش‌های سایبری ج.ا.ایران

طی یک بازه زمانی تقریباً شش‌ساله، ج.ا.ایران هدف حملات سایبری متعدد و متنوعی قرار گرفته است. مهم‌ترین آن‌ها، حمله ویروس استاکس‌نت به تأسیسات هسته‌ای نطنز می‌باشد. در این راستا، از سال ۲۰۰٦م. به بعد، مجموعه‌ای از برنامه‌های جاسوسی و تروجان[1]های بسیار پیشرفته و پیچیده برای هدف قرار دادن سیستم‌های کامپیوتری در ج.ا.ایران به‌کار گرفته شدند. نقطه آغاز چنین حملاتی با برنامه بسیار گسترده موسوم به Flame[2] شروع شد که این برنامه در حقیقت مبنا و بستر اصلی به‌کارگیری و اجرای سایر بدافزارها نظیر DuQu[3] و بعدها Stuxnet بود. در سال ۲۰۱۱م. و ۲۰۱۲م. مطبوعات آمریکا گزارش دادند این برنامه‌ها در واقع بخشی از یک پلان رژیم صهیونیستی-آمریکایی به نام «بازی‌های المپیک»[4] است که هدف آن ایجاد وقفه و توقف کامل در برنامه‌های هسته‌ای ج.ا. ایران می‌باشد. البته ادعای آمریکایی-رژیم صهیونیستی بودن بدافزار یادشده هیچ‌گاه به صورت رسمی از سوی مقامات آمریکایی و یا رژیم صهیونیستی تأیید نشد.

در سال ۲۰۰۹م. و ۲۰۱۰م. گمانه‌هایی دال بر این مطرح شد که یک ویروس رایانه‌ای تحت عنوان استاکس‌نت توسط یک دولت بزرگ ایجاد شده است تا بتواند سانتریفیوژهای نیروگاه هسته‌ای ج.ا.ایران را که می‌تواند برای غنی‌سازی اورانیوم استفاده شود، از بین ببرد. این ویروس را دولت‌های ایالات‌متحده و رژیم صهیونیستی طراحی کرده بودند و یک

1. Trojans

۲. ویروس Flame یک برنامه بسیار پیچیده و خرابکارانه بود که به صورت فعال و به عنوان یک سلاح سایبری برای هدف قرار دادن مراکز خاصی در کشورهای مختلف استفاده گردید.

۳. بدافزار پیچیده‌ای است که در سال ۲۰۱۱م. کشف شده است. این بدافزار در حملات جمع‌آوری هوشمند اطلاعات در حوزه اهداف صنعتی مورد سوء استفاده قرار گرفته بود.

4 .Olympic Games

خطای برنامه‌نویسی باعث شد تا از طریق اینترنت در سراسر جهان پخش شود (براد و همکاران[1]، ۲۰۱۹).

بیش از ۱۵ مورد از تأسیسات ج.ا.ایران توسط این ویروس مورد حمله قرار گرفتند. عقیده بر این است که این حمله توسط درایو (USB) برخی کارکنان آغاز شده است. یکی از تأسیساتی که تحت تأثیر این ویروس قرار گرفت، تأسیسات نطنز بود که در سال ۲۰۱۰م. اولین علائم آن مشخص شد. بازرسان آژانس بین‌المللی انرژی هسته‌ای ضمن بازدید از تأسیسات مشاهده کردند تعدادی از سانتریفیوژهای غنی‌سازی در حال از کار افتادن هستند. علت امر در آن موقع ناشناخته بود. پس‌ازآن، تکنسین‌های ایرانی با متخصصان امنیت رایانه بلاروسی برای بررسی سیستم‌های رایانه‌ای خود قرارداد بستند. این شرکت امنیتی سرانجام فایل مخرب را در سیستم‌های رایانه ج.ا.ایران کشف کردند. متعاقباً فاش گردید این فایل‌های مخرب، ویروس استاکس‌نت بوده است. اگرچه ج.ا.ایران جزئیات خاصی در مورد اثرات این حمله منتشر نکرد، اما تخمین زده می‌شود که این ویروس ۹۸٤ سانتریفیوژ را از کار انداخته است (کسلر[2]، ۲۰۱۱).

ج.ا.ایران طی سال‌های اخیر، تلاش‌های جدی و فراوانی را جهت تقویت و گسترش توانمندی‌های خود در حوزه فناوری اطلاعات و به‌طور کلی، حوزه سایبری به‌عمل آورده است. نمونه عملی و بارز چنین تلاشی، تشکیل شورای عالی فضای مجازی کشور به دستور و فرمان رهبر معظم انقلاب اسلامی در تاریخ ۱۷ اسفند ۱۳۹۰ است که فعالیت‌های مربوط به قلمرو سایبری را شناسنامه‌دار و ساختارمند نموده است.

علاوه بر تأسیس نهاد مذکور، رهبر انقلاب اسلامی با ابلاغ سیاست‌های کلی برنامه ششم توسعه کشور در تاریخ ۹ تیر ۱۳۹٤ در بخش مربوط به امور دفاعی و امنیتی نیز در دو بند مجزا و مشخص بر تأمین امنیت سایبری کشور و همچنین تقویت قدرت دفاع سایبری در سطح ملی تأکید نمودند که می‌توان آن را به عنوان سند چشم‌انداز و استراتژی ج.ا.ایران در حوزه فضای سایبر تلقی کرد.

1. Broad, W.J.; Markoff, J.; & Sanger, D.E.
2. Kesler, B.

از نظر هنجارسازی و تعریف مفاهیم و اصطلاحات سایبری (البته سند یا اطلاعات مشخصی که بتوان آن را مورد اشاره قرار داد) اطلاعات زیادی وجود ندارد. با این حال، کشور ایران در عرصه عمل و در قالب نیروهای مسلح اقداماتی چند را تا به امروز انجام داده است که از شکل این اقدامات و اهداف مشخص‌شده برای آن‌ها می‌توان رویه و رویکرد عملی کشور را در قبال موضوع تهدیدهای سایبری و مواجهه با آن‌ها استنباط نمود.

ج.ا.ایران در سال ۱۳۹۰ تشکیل فرماندهی سایبری نیروهای مسلح را رسماً اعلام نمود که هدف از تشکیل آن را دفاع در برابر حملات سایبری و همچنین مرکزیت بخشیدن به عملیات سایبری عنوان کرد. بنابر اظهارات مقامات رسمی کشور، فرماندهی سایبری مذکور جنبه تدافعی داشته و صرفاً برای دفع و مقابله با حملات و تهدیدهای سایبری علیه کشور به‌وجود آمده است.

علاوه‌بر این، در ساختار سپاه پاسداران انقلاب اسلامی نیز واحدی تحت عنوان سازمان پدافند غیرعامل تأسیس شده است که بعضاً از آن به عنوان دومین ارتش سایبری دنیا یاد می‌شود. علاوه‌بر این، در سطح ملی و داخلی نیز پلیس سایبری جهت تعقیب و پیگیری مجرمان رایانه‌ای نیز در ساختار نیروی انتظامی ایجاد شد که کارویژه آن، داخلی است و بُعد کیفری دارد.

٥-٤. تجزیه‌وتحلیل استراتژی امنیت سایبری آمریکا، چین و روسیه

در این بخش استراتژی امنیت سایبری آمریکا، چین و روسیه مورد تجزیه‌وتحلیل قرار خواهد گرفت. این داده‌های تحلیل‌شده به معیارهایی تقسیم می‌شوند که این اطلاعات با استراتژی امنیت سایبری ج.ا.ایران مقایسه خواهند شد.

البته هرچند نمی‌توان از اختلافات استراتژیک جلوگیری کرد؛ اما مشخص شده است که هر کشور با چه تهدیداتی مواجه است و برای ایمن نگه داشتن فضای سایبر از چه استراتژی‌هایی باید بهره گرفت. استراتژی کشورهای پیشرو، شیوه‌هایی را مشخص می‌کند و بهترین معیارها را فراهم می‌کند که در لیست‌های زیر اشاره شده است.

جدول شماره ٤. ارتقای تحقیق و توسعه امنیت سایبری	
کشور	ارتقای تحقیق و توسعه امنیت سایبری
ایالات متحده	۱. سرعت بخشیدن به تحقیقات و توسعه نوآورانه برای ایجاد قابلیت‌های سایبری، ۲. تمرکز بر توسعه قابلیت‌های سایبری جهت گسترش CMF و نیروی کار سایبری گسترده‌تر در نیروهای مسلح.
چین	۱. برای اهداف حفظ و بهبود تحقیق و توسعه چین، تحقیقات و آزمایش‌هایی برای شناسایی حملات سایبری و تجزیه و تحلیل پیشرفته انجام می‌شود. ۲. چین برای بهبود عملکرد شناسایی حملات سایبری و عملکرد تجزیه و تحلیل پیشرفته در مؤسسات تحقیقاتی، برای بهبود تحقیق و توسعه و آزمایش‌های عملی اقداماتی را انجام خواهد داد. ۳. ارتقای تحقیق و توسعه امنیت سایبری از طریق ایجاد نهادهای تخصصی در سازمان‌های حساس و حیاتی.
روسیه	۱. بخش تحقیق و توسعه در روسیه توسعه قابل‌توجهی در همه بخش‌ها طی سالیان آینده را تجربه خواهد کرد. پیش‌بینی می‌شود بخش مهندسی تحقیق و توسعه در صنعت فناوری اطلاعات روسیه با رشد ١٤ درصدی در سال ۲۰۲۰م. به ٤٢ میلیارد دلار برسد. ۲. انجام برنامه‌های تحقیق و توسعه برای رسیدگی به کلیه جنبه‌های توسعه با اهداف کوتاه مدت، میان‌مدت و بلندمدت از جمله توسعه اعتماد، آزمایش، استقرار و نگهداری آن در چرخه زندگی. ۳. انتقال، تجاری‌سازی و تبدیل آسان خروجی‌های تحقیق و توسعه برای استفاده در بخش‌های خصوصی و عمومی.
اولویت‌های پیشنهادی به ج.ا.ایران	۱. در اولویت قرار دادن تحقیق و توسعه ملی امنیت سایبری، ۲. مشارکت پشتیبانی مالی تحقیق و توسعه با نهادهای دیگر برای ایجاد نسل جدیدی از فناوری‌های ایمن.

در جدول (۵)، ارتقای آموزش امنیت سایبری در سه کشور مذکور مورد اشاره قرار گرفته است و پیشنهاداتی برای ج.ا.ایران ارائه گردید.

جدول شمار ۵. ارتقای آموزش امنیت سایبری	
کشور	ارتقای آموزش امنیت سایبری
ایالات‌متحده	۱. توسعه نیروهای مأموریت سایبری، ۲. این سیاست را برای حمایت از ابتکار ملی برای آموزش سایبری گسترش خواهد داد،

	۳. برداشتن گام‌هایی برای کمک به کشورهایی که خواهان دانش ضروری، منابع و آموزش هستند. این برنامه انواع مختلفی از برنامه‌ها را برای کمک سایر کشورها جهت دستیابی به منابع و مهارت‌ها ترتیب داده است. ٤. افزایش توانایی دولت در مبارزه با جرائم سایبری همانند آموزش نیروی انتظامی، متخصصان، پزشکی قانونی و... .
چین	۱. افزایش فعالیت‌های آگاهی‌بخشی از مراحل مدارس ابتدایی، متوسطه و اجرای پروژه‌های آگاهی بخشی مشارکتی، ۲. ارتقای فعالیت‌های داوطلبانه نهادهای خصوصی و سازمان‌های آموزشی، ۳. آگاه کردن مردم از آگاهی‌بخشی امنیت سایبری، ٤. اقدام لازم جهت حفاظت از زیرساخت‌های حیاتی، ایجاد موسسه‌ای برای ارزیابی و صدور گواهی‌نامه برای سیستم‌های کنترل صنعتی، افزودن مقوله‌های بیشتر اگر حملات سایبری تأثیر قابل‌توجهی در زندگی شهروندان داشته باشند.
روسیه	۱. اجرای چندین برنامه آگاهی و آموزش در مورد جرائم سایبری برای نهادهای اجرایی قانون، ۲. تقویت بخش رسمی و غیررسمی برنامه‌های آموزشی برای حمایت از نیازهای امنیت سایبری و ایجاد ظرفیت، ۳. ایجاد آزمایشگاه‌های مفهوم امنیت سایبری برای ایجاد آگاهی و پیشرفت در مناطق کلیدی، ٤. ترویج و راه‌اندازی یک برنامه جامع آگاهی ملی در مورد امنیت فضای سایبر.
اولویت‌های پیشنهادی به ج.ا.ایران	۱. افزایش توانایی متخصصان امنیت سایبری در زمینه مدیریتی، فنی و اطلاعاتی، ۲. افزودن آگاهی در مورد امنیت سایبری به برنامه‌های درسی آموزش ملی به عنوان روشی برای گسترش دانش به دانش آموزان و بستگان آن‌ها، ۳. سرمایه‌گذاری در بخش آموزش و تحقیقات بنیادی امنیت سایبری، ٤. آموزش سیاست‌گذاران ارشد، مسئولان دولتی در مورد تهدیدات شبکه‌های الکترونیکی، ۵. برای افزایش آگاهی در مورد تهدیدات سایبری یک برنامه ملی باید وجود داشته باشد.

در جدول (٦)، اطمینان از تشخیص خطرات حاضر در زمینه سایبر در سه کشور مذکور مورد اشاره قرار گرفته است و پیشنهاداتی برای ج.ا.ایران ارائه گردید.

جدول شماره ٦. اطمینان از تشخیص خطرات حاضر

کشور	اطمینان از تشخیص خطرات حاضر
ایالات‌متحده	۱. شناسایی تهدیدها قبل از آن‌که بتوانند امنیت ملی ایالات‌متحده را تحت تأثیر قرار دهند،

	وزارت دفاع به گسترش و تحقق این راه‌حل‌ها از طریق نظارت مداوم بر شبکه، بهبود آموزش برای نیروی کار روش‌های بهینه برای شناسایی، گزارش‌دهی و ردیابی رفتارهای مشکوک ادامه می‌دهد. ۲. برای نظارت، هشدار و پاسخ به حادثه از طریق تبادل اطلاعات با شبکه‌های قابل‌اعتماد شرکای بین‌المللی، ایالات‌متحده مشارکت فعال خواهد داشت. ۳. با اجرای سیاست‌ها، پروتکل‌ها و ایجاد فرهنگ آگاهی‌بخشی برای پیش‌بینی، کشف و پاسخ به تهدیدات پیش از تأثیرگذاری انجام خواهد شد.
چین	۱. شناسایی و اولویت‌بندی خطرات سایبری و از طریق ارزیابی ریسک، آسیب‌پذیری و بررسی سیستم، ۲. پیاده‌سازی یک برنامه محافظت با فرایندهای مدیریت ریسک سایبری قوی و منظم در تمام بخش‌های مهم، ۳. اندازه‌گیری مداوم عملکرد از طریق فرایند تمرینات سایبری.
روسیه	۱. ایجاد بهترین شرایط برای اجرای فرایندهای رسمی ارزیابی ریسک، مدیریت ریسک، مدیریت بحران که برای کاهش خطر اختلال و بهبود وضعیت امنیتی برنامه‌ریزی‌شده است، ۲. ایجاد آگاهی از تهدیدات، آسیب‌پذیری‌ها و عواقب امنیتی در بین اشخاص برای مدیریت خطرات زنجیره خطرات مرتبط با IT (تولیدات، سیستم‌ها و یا خدمات).
اولویت‌های پیشنهادی به ج.ا.ایران	۱. تقویت مقاومت زیرساخت‌های اطلاعات حیاتی، ۲. تمرکز بر مقابله با تهدیدات که به احتمال زیاد مانع انجام مأموریت سازمان‌های دولتی و مشاغل می‌شود. ۳. همکاری دولت با بخش خصوصی برای مشارکت گسترده‌تر تجزیه و تحلیل، هشدار، جمع‌آوری اطلاعات، کاهش آسیب‌پذیری و بازیابی، ٤. تدوین روشی برای به اشتراک‌گذاری اطلاعات در مورد حملات سایبری، تهدیدات و آسیب‌پذیری‌ها با اقصی نقاط جهان، ۵. تأمین ظرفیت پاسخ‌گویی به حوادث مهم ملی در صورت حملات مهم به زیرساخت‌های مهم.

در جدول (۷)، ارتقای سیاست مقابله با جرائم سایبری در سه کشور مذکور مورد اشاره قرار گرفته است و پیشنهاداتی برای ج.ا.ایران ارائه گردید.

جدول شماره ۷. ارتقای سیاست مقابله با جرائم سایبری

کشور	ارتقای سیاست مقابله با جرائم سایبری

ایالات‌متحده	۱. وزارت دفاع بهترین اقدامات را برای مقابله با گسترش بدافزارهای مخرب در سیستم بین‌الملل در همکاری با وزارت امور خارجه و سپس با شرکای بین‌المللی اتخاذ خواهد کرد. ۲. وزارت دفاع با همکاری جامعه اطلاعاتی برای توسعه داده‌ها، پایگاه اطلاعات، الگوریتم‌ها و قابلیت‌های مدل‌سازی و شبیه‌سازی، برای اثربخشی عملیات سایبری همکاری خواهد کرد. ۳. حفاظت از مالکیت معنوی از جمله اسرار تجاری در برابر سرقت و جاسوسی.
چین	۱. اتحادیه آموزش و اقدام سایبری چین اقدام لازم جهت به اشتراک‌گذاری اطلاعات را از طرق همکاری با بخش خصوصی از جمله شورای جلوگیری از ارتباطات غیرمجاز، را انجام خواهد داد. ۲. چین کنوانسیون مربوط به جرائم سایبری را تصویب کرده است و برای تقویت تحقیقات متقابل سریع و مؤثر بین نهادها تلاش خواهد کرد.
روسیه	۱. پیشگیری هنوز استراتژی کلیدی برای مقابله با جرائم سایبری است و اولویت با آموزش و توانمندسازی مردم است. ۲. امن‌تر کردن جامعه و فضای کسب‌وکار با مبارزه با جرائم سایبری و محافظت از داده‌های شخصی.
اولویت‌های پیشنهادی به ج.ا.ایران	۱. تجهیز جامعه و کسب‌وکار برای ایجاد فضای سایبری امن‌تر با مقابله مداوم با تهدیدات و محافظت از داده‌های شخصی، ۲. برای ایجاد یک شبکه جامع اینترنت ملی، مبنای حقوقی را تعریف می‌کند. برای مثال اختیار از کار انداختن زیرساخت‌های مهم را در صورت خطر حمله سایبری تعیین می‌کند. ۳. ارتقای قابلیت‌های قانون در تحقیقات، پیشگیری و پیگرد قانونی جرائم سایبری.

در جدول (۸) ارتقای سیاست مقابله با جرائم سایبری در سه کشور مذکور مورد اشاره قرار گرفته است و پیشنهاداتی برای ج.ا.ایران ارائه گردید.

جدول شماره ۸. مقایسه در ارتقای امنیت سایبری در حقوق بین‌الملل

کشور	ارتقای امنیت سایبری در حقوق بین‌الملل
ایالات‌متحده	۱. وزارت دفاع اتحادها و مشارکت‌های بین‌المللی خود را برای توسعه توانایی‌های اشتراکی در دستابی به تأثیر بیشتر تقویت می‌کند. ۲. این کار با همکاری شرکای توانمند بین‌المللی برای برنامه‌ریزی و آموزش و اجرای عملیات سایبری انجام می‌شود.
چین	۱. برای تأمین ثبات در استفاده از فضای مجازی، همکاری‌های بین‌المللی را ارتقا می‌بخشد و چارچوبی را چین ایجاد می‌کند که به‌طور فعال در اجرای قوانین بین‌المللی شرکت کند.

	۲. چین کنوانسیون مربوط به جرائم سایبری را تصویب کرده است و برای تقویت تحقیقات متقابل سریع و مؤثر بین نهادها تلاش خواهد کرد.
روسیه	۱. روسیه نسبت به مشارکت بین‌المللی در حوزه ایجاد قوانین سایبری چندان خوش‌بین نیست لذا بر ارتقای امنیت و قوانین سایبری خود تکیه کرده است.
اولویت‌های پیشنهادی به ج.ا.ایران	۱. برای تدوین مواضع بین‌المللی امنیت سایبری ج.ا.ایران، شورای هماهنگ‌کننده امنیت سایبری باید شکل گیرد که با نهادها و ادارات دولتی و خصوصی و دانشگاه‌ها باید همکاری کند.

در جدول (۹) مقایسه اشکال قانونی و جنبه‌های نهادی در سه کشور مذکور به همراه ج.ا.ایران مورد اشاره قرار گرفته است.

جدول شماره ۹. مقایسه اشکال قانونی و جنبه‌های نهادی

کشور	اشکال قانونی و جنبه‌های نهادی
ایالات‌متحده	۱. تقویت امنیت سایبری، از طریق مقررات و تلاش‌های مشترک بین دولت و بخش خصوصی، که پیشرفت‌های داوطلبانه را در امنیت سایبری پرورش می‌دهد. ۲. با مطالبه شرکت‌ها برای بهبود امنیت سایبری، کنگره همچنین در نظر دارد تا لوایحی را در خصوص جرم شناختن حملات سایبری برای پاسخ به توسعه امنیت سایبری شرکت‌ها تصویب کند.
چین	۱. برای نهادی متنوعی همچون دولت، بخش‌های دولتی، دانشگاهی، صنعتی و خصوصی در چین لازم است که هر نهاد اقدامات امنیتی اطلاعات خود را به روشی مستقل و فعالانه به‌عنوان بخشی از مسئولیت‌های اجتماعی خود انجام دهد. ۲. چین برای ایجاد فضای امن و قابل اعتماد تلاش کرده است که در آن جریان آزاد اطلاعات تضمین‌شده باشد. ۳. تقویت بنیادی مردم در ارتباط با فضای مجازی. ٤. اپراتورهای فضای مجازی بازار ایجاد خواهد کرد از طریق توسعه پیشرفته فن‌آوری‌ها و محصولات، تربیت منابع انسانی با توانایی بالا و استفاده از منابع برای اقدامات امنیتی اطلاعات به منظور تقویت رقابت بین‌المللی صنعت امنیت سایبر چین.
روسیه	۱. بازرسی دوره‌ای و ارزیابی کفایت و اثربخشی امنیت زیرساخت‌های اطلاعاتی. ۲. فعال کردن، آموزش و تسهیل آگاهی از چارچوب نظارتی.
ج.ا.ایران	۱. هماهنگی قوانین جرائم سایبری در زمینه جرائم سایبری به همکاری بین‌المللی کمک و به مسائل قضایی رسیدگی می‌کند.

	۲. قانون جرائم سایبری باید توسط سازمان‌های خصوصی محلی، دانشگاهیان، شهروندان و تمامی کسان دیگری که منافع شناخته‌شده دارند، ارزیابی شود. ۳. قانون جرائم سایبری ملی مطابق با کنوانسیون جرائم سایبری باشد.

در جدول (۱۰) مقایسه موازنه امنیت سایبری و آزادی‌های مدنی در سه کشور مذکور به همراه پیشنهاداتی برای ج.ا.ایران مورد اشاره قرار گرفته است.

جدول شماره ۱۰. مقایسه موازنه امنیت سایبری و آزادی‌های مدنی

کشور	موازنه امنیت سایبری و آزادی‌های مدنی
ایالات‌متحده	۱. وزارت دفاع چارچوبی را برای کمک به دفاع از دولت فدرال و بخش خصوصی تهیه می‌کند که با همراهی مقامات مدنی در حمایت از DHS و سایر آژانس‌ها و مقامات ایالتی انجام می‌شود. ۲. اولویت با حفظ، تقویت و ارتقای دسترسی به اینترنت آزاد جهانی است. ۳. تشویق همکاری‌های بین‌المللی برای محافظت داده‌های تجاری. ٤. تقویت مسیرهای شغلی پایدار برای کلیه کارکنان نظامی که عملیات سایبری را انجام و پشتیبانی می‌کنند.
چین	۱. تأکید بر اهمیت همکاری و مشارکت با سایر ملل و مناطقی که دارای ارزش‌های یکسانی در سیاست، دموکراسی، احترام به حقوق بشر و حاکمیت قانون است. به همین دلیل، دیپلماسی‌ای لازم است که با ایجاد رویکردی متعادل از ایجاد فضای مجازی ایمن اطمینان حاصل کند. ۲. فضای مجازی مزایایی را ازجمله نوآوری، رشد اقتصادی و راه‌حل‌های مربوط به موضوعات اجتماعی را در اختیار ما قرار داده و درعین‌حال از آزادی بیان و حریم خصوصی محافظت می‌کند.
روسیه	۱. تشویق به استفاده از استانداردهای باز برای تسهیل قابلیت‌های همکاری و تبادل داد در بین تولیدات یا خدمات مختلف. ۲. برای افزایش دسترسی به محصولات آزمایش‌شده و دارای مجوز بر اساس استانداردهای باز، یک کنسرسیوم دولتی و خصوصی تقویت خواهد شد. ۳. تسهیل شناسایی، اولویت‌بندی، ارزیابی، اصلاح و محافظت از زیرساخت‌های مهم و منابع اصلی مبتنی بر برنامه حفاظت.
اولویت‌های پیشنهادی به ج.ا.ایران	۱. نوآوری در امنیت سایبری به توسعه راه‌حل‌های بلندمدت کمک می‌کند. ۲. تعریف و اجرای چارچوب محکم احراز هویت توسط دولت.

در جدول (۱-۱۱) مقایسه انواع همکاری‌ها: بستر خصوصی-عمومی مرتبط با حوزه سایبری در سه کشور مذکور به همراه پیشنهاداتی برای ج.ا.ایران مورد اشاره قرار گرفته است. در جداول مرتبط بعدی، به ترتیب به مقایسه انواع همکاری‌های درون حکومتی و همکاری منطقه‌ای اشاره شده است.

جدول شماره ۱-۱۱. مقایسه انواع همکاری‌ها: بستر خصوصی-عمومی

کشور	بستر خصوصی-عمومی
ایالات‌متحده	سایر نهادها ایجاد خواهد کرد. وزارت دفاع در همکاری با FBI,CIA,DHS و آژانس‌های دیگر برای ایجاد روابط و ادغام قابلیت‌ها همکاری خواهد کرد تا رئیس‌جمهور گزینه‌های مختلف را در پاسخ به حملات سایبری در اختیار داشته باشد.
چین	۱. همکاری با متحدین حول محور چین ۲. نظارت بر همکاری شرکت‌های خصوصی با شرکای خارجی به خصوصی در حوزه فناوری‌های اطلاعاتی
روسیه	۱. همگرایی با کشورهای توسعه‌یافته و درحال توسعه، سازمان‌های چندجانبه برای به اشتراک‌گذاری دانش البته با در نظر گرفتن مسائل امنیتی و حفظ محوریت روسیه. ۲. اجرای پروژه‌های در سطح جهانی برای نمایش قدرت. ۳. ظرفیت‌سازی و به اشتراک‌گذاری تخصص در زمینه‌هایی مانند حاکمیت، حاکمیت اینترنت و ... .
اولویت‌های پیشنهادی به ج.ا.ایران	برای تسهیل اشتراک دارایی‌های امنیت سایبری در سراسر مرزها یا کشورهای دیگر، جمهوری اسلامی ایران نیاز به همکاری‌های رسمی با برخی سازمان‌های بین‌المللی دارد.

جدول شماره ۲-۱۱. مقایسه انواع همکاری‌ها: همکاری درون حکومتی

کشور	همکاری درون حکومتی
ایالات‌متحده	۱. با ارتقای به‌موقع جریان اطلاعات بین DHS و شرکت‌های مهم زیرساخت، مشارکت‌های میان دولت و بخش خصوصی بهبود میابد. ۲. بهبود فرایندها از بخش دولتی گرفته تا خصوصی تا بتوانند به اطلاعات حساس و طبقه‌بندی شده دسترسی داشته باشند.
چین	بسیاری از ذینفعان در فضای مجازی باید ضمن آنکه نقش مربوط به خود در جامعه را انجام

	می‌دهند، به همکاری و کمک متقابل با یکدیگر ازجمله همکاری‌های بین‌المللی و بخش خصوصی بپردازند.
روسیه	۱. تسهیل و همکاری بین نهادهای ذینفع از جمله بخش خصوصی برای اقدامات مربوط به تهدید سایبری، آسیب‌پذیری نقص و اتخاذ بهترین اقدام. ۲. ایجاد یک اتاق فکر برای بحث و گفت‌وگو درباره سیاست امنیت سایبری.
اولویت‌های پیشنهادی به ج.ا.ایران	۱. کار و تمرین مشترک در دوره‌های آموزشی که می‌تواند کمبود متخصصان ماهر امنیت سایبری را کاهش دهد. ۲. فراهم کردن امکان تبادل اطلاعات در مورد تهدیدات و آسیب‌پذیری سایبری. ۳. برگزاری نشست با نهادهای اجرای قانون، صنعتی و آکادمی‌ها برای به اشتراک گذاشتن دانش.

جدول شماره ۳-۱۱. مقایسه انواع همکاری‌ها: همکاری منطقه‌ای

کشور	همکاری منطقه‌ای
ایالات‌متحده	ایجاد مشارکت استراتژیک جدید در منطقه آسیا-پاسفیک با همکاری وزارت دفاع برای ایجاد ظرفیت سایبری و به حداقل رساندن خطر برای ایالات‌متحده و منافع متحدین.
چین	این کشور به طور فعال در بحث‌ها و جلسات چندجانبه از جمله نهادهای منطقه‌ای و سایر کمیته‌های مرتبط در سازمان ملل متحد شرکت خواهد کرد.
روسیه	۱. اطمینان حاصل شود که منافع استراتژیک و اقتصادی در گفت‌وگوهای دوجانبه و چندجانبه مورد توجه قرار می‌گیرد. ۲. همکاری با ملت‌های همفکر و نهادهای جهانی برای ایجاد هنجار و رفتار قابل‌قبول برای فعالیت در فضای مجازی.
ج.ا.ایران	ج.ا.ایران در راستای ارتقای امنیت سایبری و با هدف تشکیل سازمان‌های تخصصی سایبری، باید هرچه سریع‌تر با همسایگان خود وارد گفت‌وگو شود.

برای درک بهتر مقایسه‌های مذکور، معیارهایی در جدول (۱۲) ارائه شده است.

جدول شماره ۱۲. معیارهایی برای درک بهتر مقایسه سیاست‌های سایبری

معیار مقایسه	وضعیت معیار	آمریکا	چین	روسیه	ج.ا.ایران
۱. ارتقای تحقیق و توسعه امنیت سایبری	موجود	√	√	√	
	تاحدودی موجود				√
	ناموجود				

۲. اطمینان از تشخیص خطرات حاضر		موجود	√	√	√	√
		تاحدودی موجود				
		ناموجود				
۳. ارتقای آموزش امنیت سایبری		موجود	√	√		√
		تاحدودی موجود			√	
		ناموجود				
٤. ارتقای سیاست مقابله با جرایم سایبری		موجود	√			
		تاحدودی موجود		√	√	√
		ناموجود				
۵. ارتقا امنیت سایبری در حقوق بین‌الملل		موجود	√			
		تاحدودی موجود		√		√
		ناموجود			√	
٦. اشکال قانونی و جنبه‌های نهادی		موجود	√	√	√	√
		تاحدودی موجود				
		ناموجود				
۷. موانه امنیت سایبری و آزادی های مدنی		موجود	√	√	√	
		تاحدودی موجود				√
		ناموجود				
۸. انواع همکاری	الف. بستر خصوصی- عمومی	موجود	√	√		√
		تاحدودی موجود			√	
		ناموجود				
	ب. همکاری درون حکومتی	موجود				
		تاحدودی موجود	√	√	√	√
		ناموجود				
	پ. همکاری منطقه‌ای	موجود				
		تاحدودی موجود	√	√	√	
		ناموجود				√
	ت. همکاری بین حکومتی	موجود	√	√	√	√
		تاحدودی موجود				
		ناموجود				

۵. نتیجه‌گیری و پیشنهادات

در مقایسه راهبردهای امنیتی سایبری کشورهای دیگر مشخص می‌شود که در برخی از معیارها، ج.ا.ایران در شرایط خوبی قرار دارد اما در برخی دیگر، هنوز جای پیشرفت بسیاری وجود دارد. استراتژی آن تاحدودی در ارتقای آموزش امنیت سایبری، ارزیابی خطرات فعلی، سیاست مقابله با جرایم سایبری، اشکال مقررات و انواع همکاری‌ها قوی است. با این‌حال، جای کار بسیاری هنوز در بخش تحقیق و توسعه، هماهنگی با قوانین بین المللی، توازن بین امنیت و آزادی‌های مدنی و همکاری‌های منطقه‌ای وجود دارد. با توجه به چالش‌های مطرح‌شده، برای مواجهه مناسب با فضای سایبر، برخی از راه‌کارهای زیر پیشنهاد می‌شود. البته این مباحث بایستی به خبرگان ارائه و نظرات آن‌ها گردآوری شود.

(۱) ایجاد استانداردهای جدید و توافق‌نامه‌های تجاری با نهادهای جدید،

(۲) تعریف مشاغل جدید و آموزش افراد،

(۳) وضع قوانین و مقررات مورد نیاز در حوزه‌های مختلف مرتبط با فضای سایبر در سطح ملی و بین‌المللی،

(٤) داشتن افراد و پرسنل آموزش و تعلیم‌دیده در زمینه حوزه سایبر و مسائل مرتبط با آن،

(۵) داشتن اینترنت ملی و قطع وابستگی به اینترنت کشورهای سلطه‌گر،

(٦) داشتن یک فرماندهی و کنترل واحد برای رهبری و هدایت فضای سایبر در سطح ملی و بین‌المللی،

(۷) داشتن بسیج سایبری برای محتواسازی مستمر بر اساس ارزش‌های اسلامی و ایرانی،

(۸) توانایی ائتلاف‌سازی سایبری با کشورها و گروه‌های جبهه مقاومت و کشورهای دوست و همراه،

(۹) راه‌اندازی رشته‌های مختلف در حوزه علوم انسانی، علوم شناختی، امنیتی-دفاعی مرتبط با فضای سایبر مانند:

- جامعه‌شناسی سایبری،
- روانشناسی سایبری،
- حقوق و روابط بین‌الملل سایبری،
- فقه سایبری،
- تکنولوژی‌های آموزشی سایبرمحور،
- مدیریت مالی و پولی سایبرمحور،
- سبک زندگی در فضای سایبر،
- آموزش و پرورش سایبرمحور،
- استانداردسازی سایبرمحور و... .

(۱۰) مردمی‌کردن امنیت سایبری و سرشکن کردن هزینه‌های مرتبط با آن،

(۱۱) تلاش برای هرچه مخفی‌تر و گمنام‌تر ماندن عملیات‌های سایبری،

(۱۲) تمرکز بر تربیت کودکان، نوجوانان و جوانان بر اساس محیط زندگی سایبری و ارزش‌های اسلامی و ایرانی،

(۱۳) ایجاد صنایع دفاعی سایبری (یا سایبر الکرونیک)،

(۱٤) تدوین اصول جنگ ترکیبی/ نامتقارن/ مردم‌محور سایبرمحور (بر اساس آیه «وأعدوا لهم ما آستطعتم من قوة»)،

(۱۵) تاب‌آور نگهداشتن سامانه‌ها/ اطلاعات/ زیرساخت‌های ملی و بین‌المللی مرتبط (مستقیم و غیرمستقیم) با امنیت ملی،

(۱٦) تلاش برای کاهش و سپس قطع وابستگی سخت‌افزاری و نرم‌افزاری به دیگران،

(۱۷) ایجاد آزمایشگاه‌های تست و صحت‌سنجی سخت‌افزارها و نرم‌افزارهای وارداتی و توجه جدی در سطح ملی به آن،

(۱۸) ایجاد نهضت سوادآموزی سایبری برای عقب‌ماندگان سایبری در کشور و توانمند کردن آن‌ها جهت استفاده اثربخش از خدمات سایبری بخصوص از

طریق گوشی‌های هوشمند همراه (به‌خصوص با استفاده از دانش‌آموزان جهت آموزش پدر و مادرها و اقوام)،

(۱۹) طراحی پول دیجیتالی ملی و قوانین و مقررات آن.

اگرچه این مطالعه نشان داد استراتژی امنیت سایبری جمهوری اسلامی ایران در وضعیت امیدوار کننده‌ای قرار دارد اما با اجرای بخش‌های مختلف و رفع نواقص ذکر شده می‌توان گفت که به شرایط ایده‌آل رسیده است. با این حال، راه‌کارها اگر کاربردی و عملیاتی نشود، صرفاً یک سند است. فقط اجرای صحیح این موارد است که می تواند کشور را از فضای خصمانه در امان نگه دارد؛ اگرچه این پژوهش خواستار ارزیابی استراتژی امنیت ملی سایبری ج.ا.ایران و ارائه پیشنهادهایی برای بهبود آن است، اما قابلیت اطمینان و سازگاری آن به پژوهش‌ها و تحقیقات آتی سپرده می‌شود.

منابع

الف- فارسی

- انوشا، سهیل؛ نیکجو، مهنوش؛ و کولیوند، روح‌اله (۱۴۰۰)، «استراتژی امنیت سایبری» (صص: ۱۹۹-۲۰۶)، ***مجموعه مقالات سومین همایش ملی تحقیقات میان‌رشته‌ای در علوم مهندسی و مدیریت***، تهران: موسسه پژوهشی مدیریت مدبر.
- بیابانی، غلامحسین؛ هادیانفر، سید کمال (۱۳۸۴). ***فرهنگ توصیفی علوم جنایی***. تهران: انتشارات مرکز تحقیقات کاربردی کشف جرائم و امنیت معاونت آگاهی ناجا، چاپ اول.
- رهامی، روح‌الله؛ اژدری، امیرحسین (۱۴۰۱). «امنیت سایبری اتحادیه اروپا: تهدیدات، فرصت‌ها و اقدام»، ***فصلنامه تحقیقات حقوقی*** (ویژه‌نامه حقوق و فناوری)، ۲۵ (۹۹)، ۲۷۳-۳۰۲.

ب- انگلیسی

- Broad, W.J.; Markoff, Jand Sanger, D.E. (2011). "IsraeliTestonWormCalledCrucialinIranNuclearDelay", ***The new York Tims***, Jan 15, viewed 28 December 2019, At: https://www.nytimes.com.
- CEU School of Public Policy (2017). ***Understanding Russia's Internet Policy***. [online] Availableat: https://cmds. Ceu.edu/article/2017-03-16/understanding -Russias-internet -policy.
- Congressional Executive Commissionon China (2005). ***Provisionsonthe Administrationo fInternet News Information Services*** (Chinese Text and CECC Full Translation. [online] Available at: https://www.cecc.gov/resources/legal-provisions/provisions-on-the-administration – of -internet-news-informationservices.
- Dou, E. (2017). "JailedforaText: China's Censors Are Spying on Mobile Chat Groups", ***The WallStreet Journal***, [online] Available at: https://www.wsj.com/articles/jailed-for-a-text-chinas-censors-are-spying-on-mobile-chatgroups-1512665007
- Dowell, W. (2006). "The Internet, censorship and China", ***Georgia Journal of International Affairs***, 7 (2), 111-119.
- FreedomHouse (2018). ***Freedom on the Net 2018: China Country Report***, Freedom House, [online] Available At: https://freedomhouse.org/report/freedom-net/2018/china.

- FreedomHouse (2018). ***Freedom on the Net 2018: Russia Country Report***, Freedom House, [online] Available at: https://freedomhouse.org/report/freedom-net/2018/Russia.
- James, Y.; Jones, S. (2017). "When Russian Trolls Attack", In: ***Wired***, [online] Available at: https://www.wired.com/2017/10/russian-trolls-attack/.
- Kesler, B (2011). "The Vulner ability of Nuclear Facilitiesto Cyber Attack", ***Strategic Insights***, Spring, 10(1) 15-25, At: http://large.stanford.edu/courses/2017/ph241/bunner2/docs/SI-v10-I1_Kesler.pdf.
- Lee, Don (2013). "China Dismisses U.S. Accusations of Cyber-Spying", ***Los Angeles Times***, May 7, At: http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-uscyber-spying-20130507.
- Liang, B.and Lu, H. (2010). "Internet Development, Censorship, and Cyber Crimesin China", ***Annual Review of Sociology***, 26 (1),103–20.
- Shahbaz, A. (2018). "Freedom on the Net Report 2018 The Rise of Digital Authoritarianism", [online] ***Freedom House***. Available at: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.
- Theohari, C.A.(2018). "***Information Warfare: Issues for Congress Congressional Research Service***", At: https://sgp.fas.org/crs/natsec/R45142.pdf
- USL egal (2019). ***Federal Laws Internet Law***. [online] USL egalInternet Law, Available At: https://internetlaw.uslegal.com/piracy-and-file-sharing/federal-laws/.
- Xu, B.; Albert, A. (2017). ***Media Censorshipin China***. [online] Council on Foreign Relations .Availableat: https://www.scirp.org/reference/referencespapers?referenceid=3345884.